

AMENDMENTS TO THE CLAIMS

- 1-9. (Cancelled)
10. (Previously Presented) A method as recited in Claim 33, wherein identifying first sub-entries in a first access control list comprises:
- identifying a dimensional range and a policy action for each entry in the first access control list;
 - identifying all overlapping dimensional ranges in the first access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the first access control list overlap;
 - identifying all non-overlapping dimensional ranges in the first access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the first access control list that do not overlap dimensional ranges of other entries in the first access control list;
 - identifying a policy action for each identified overlapping dimensional range in the first access control list; and
 - identifying a policy action for each identified non-overlapping dimensional range of the first access control list.
11. (Previously Presented) A method as recited in Claim 35, wherein identifying second sub-entries in a second access control list comprises:
- identifying a dimensional range and a policy action for each entry in the second access control list;
 - identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;
 - identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

identifying a policy action for each identified overlapping dimensional range of the second access control list; and
identifying a policy action for each identified non-overlapping dimensional range of the second access control list.

12-13. (Canceled)

14. (Previously Presented) A method as recited in Claim 10, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

15. (Previously Presented) A method as recited in Claim 10, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

16. (Previously Presented) A method as recited in Claim 10, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

17-32. (Cancelled)

33. (Currently Amended) A method of comparing access control lists to configure a security policy on a network, the method comprising the computer-implemented steps of:
subtracting two entries among multiple first access control entries in a first access control list from each other;
determining, from results of subtracting the two entries among the multiple first access control entries in the first access control list from each other, a set of non-overlapping representation for dimensional ranges covered by the two entries

among the multiple first access control entries in the first access control list;
identifying, based on the set of non-overlapping representation, one or more first sub-entries in ~~[[a]]~~ the first access control list, wherein the first access control list comprises ~~multiple first access control entries, and wherein the first sub-entries identified from the first access control list comprise (i) disjoint entries of the first entries or (ii) overlapping sections identified from the first entries or (iii) non-overlapping sections identified from the first entries; and~~
programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of multiple second access control entries in the second access control list.

34. (Previously Presented) A method as recited in Claim 33, further comprising determining that the first access control list is functionally equivalent to the second access control list in response to a determination that each of the first sub-entries is equivalent to or contained by one or more entries of the second access control list.
35. (Previously Presented) A method as recited in Claim 33, further comprising:
identifying second sub-entries in the second access control list, wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries; and
wherein determining whether each of the first sub-entry in the first access control list is equivalent to or contained by one or more entries of the second access control list includes determining whether the each of the first sub-entries in the first access control list is equivalent to or contained by one or more of the second sub-entries identified from the second control list.
36. (Currently Amended) A computer readable medium for comparing access control lists to configure a security policy on a network, the computer readable medium carrying

instructions for performing the steps of:

subtracting two entries among multiple first access control entries in a first access control list from each other;

determining, from results of subtracting the two entries among the multiple first access control entries in the first access control list from each other, a set of non-overlapping representation for dimensional ranges covered by the two entries among the multiple first access control entries in the first access control list;

identifying, based on the set of non-overlapping representation, one or more first sub-entries in [[a]] the first access control list, wherein the first access control list comprises multiple first access control entries, and wherein the first sub-entries identified from the first access control list comprise (i) disjoint entries of the first entries or (ii) overlapping sections identified from the first entries or (iii) non-overlapping sections identified from the first entries; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of multiple second access control entries in the second access control list.

37. (Currently Amended) A policy server communicatively coupled to security devices in a network to configure a security policy on a network, the policy server comprising:
- a processor;
 - a network interface that communicatively couples the processor to the network to receive flows of packets therefrom;
 - a memory; and
 - sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out the steps of:
 - subtracting two entries among multiple first access control entries in a first access control list from each other;
 - determining, from results of subtracting the two entries among the multiple first access control entries in the first access control list from each other, a set

of non-overlapping representation for dimensional ranges covered by the two entries among the multiple first access control entries in the first access control list;

identifying, based on the set of non-overlapping representation, one or more first sub-entries in [[a]] the first access control list, wherein the first access control list comprises multiple first access control entries, and wherein the first sub-entries identified from the first access control list comprise (i) disjoint entries of the first entries or (ii) overlapping sections identified from the first entries or (iii) non-overlapping sections identified from the first entries; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of multiple second access control entries in the second access control list.

38. (Previously Presented) A policy server as recited in Claim 37, wherein said sequence of instructions further comprising instructions for performing determining that the first access control list is functionally equivalent to the second access control list in response to a determination that each of the first sub-entries is equivalent to or contained by one or more entries of the second access control list.

39. (Previously Presented) A policy server as recited in Claim 37, wherein said sequence of instructions further comprising instructions for performing identifying second sub-entries in the second access control list, wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries; and

wherein said instructions for performing determining whether each of the first sub-entry in the first access control list is equivalent to or contained by one or more entries

of the second access control list include instructions for performing determining whether the each of the first sub-entries in the first access control list is equivalent to or contained by one or more of the second sub-entries identified from the second control list.

40. (Previously Presented) A policy server as recited in Claim 37, wherein said instructions for performing identifying first sub-entries in a first access control list comprise: instructions for performing identifying a dimensional range and a policy action for each entry in the second access control list;
instructions for performing identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;
instructions for performing identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;
instructions for performing identifying a policy action for each identified overlapping dimensional range in the second access control list; and
instructions for performing identifying a policy action for each identified non-overlapping dimensional range of the second access control list.
41. (Previously Presented) A policy server as recited in Claim 39, wherein said instructions for performing identifying second sub-entries in a second access control list comprise: instructions for performing identifying a dimensional range and a policy action for each entry in the second access control list;
instructions for performing identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;
instructions for performing identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges

corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

instructions for performing identifying a policy action for each identified overlapping dimensional range of the second access control list; and

instructions for performing identifying a policy action for each identified non-overlapping dimensional range of the second access control list.

42. (Previously Presented) A policy server as recited in Claim 40, wherein said instructions for performing identifying a dimensional range and a policy action for each entry in the first access control list include instructions for performing identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.
43. (Previously Presented) A policy server as recited in Claim 40, wherein said instructions for performing identifying a dimensional range and a policy action for each entry in the first access control list include instructions for performing identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.
44. (Previously Presented) A policy server as recited in Claim 40, wherein said instructions for performing identifying a dimensional range and a policy action for each entry in the first access control list include instructions for performing identifying a communication protocol for communication packets specified by each of the entries in the first access control list.
45. (Currently Amended) An apparatus for comparing access control lists to configure a security policy on a network, the apparatus comprising:
means for subtracting two entries among multiple first access control entries in a first access control list from each other;
means for determining, from results of subtracting the two entries among the multiple

first access control entries in the first access control list from each other, a set of non-overlapping representation for dimensional ranges covered by the two entries among the multiple first access control entries in the first access control list;

means for identifying, based on the set of non-overlapping representation, one or more first sub-entries in ~~[[a]] the first access control list, wherein the first access control list comprises multiple first access control entries, and wherein the first sub-entries identified from the first access control list comprise (i) disjoint entries of the first entries or (ii) overlapping sections identified from the first entries or (iii) non-overlapping sections identified from the first entries; and~~

means for programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of multiple second access control entries in the second access control list.

46. (Previously Presented) An apparatus as recited in Claim 45, further comprising means for determining that the first access control list is functionally equivalent to the second access control list in response to a determination that each of the first sub-entries is equivalent to or contained by one or more entries of the second access control list.

47. (Previously Presented) An apparatus as recited in Claim 45, further comprising means for identifying second sub-entries in the second access control list, wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries; and

wherein the means for determining whether each of the first sub-entry in the first access control list is equivalent to or contained by one or more entries of the second access control list includes means for instructions for performing determining whether the each of the first sub-entries in the first access control list is equivalent to or contained by one or more of the second sub-entries identified from the

second control list.

48. (Previously Presented) An apparatus as recited in Claim 45, wherein the means for identifying first sub-entries in a first access control list comprises:
- means for identifying a dimensional range and a policy action for each entry in the second access control list;
 - means for identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;
 - means for identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;
 - means for identifying a policy action for each identified overlapping dimensional range in the second access control list; and
 - means for identifying a policy action for each identified non-overlapping dimensional range of the second access control list.